

What is claimed is:

1. A system for managing files comprising a computer and a storage unit, wherein

5 the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing  
10 keys;

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key, and

15 the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are authenticated with each other, creating access  
20 allowing keys;

access allowing key group storing means for storing all the access allowing keys;

access allowing key identification means for identifying if the access allowing key sent from the  
25 file accessing means and stored in the access allowing

0958567-10504  
TOP SECRET 22958560

key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

5        secure area accessing means for accessing a secure area usually inaccessible.

2. The system for managing files according to claim 1, wherein the reciprocal authenticating means provided in said computer and said file accessing means are implemented by a unit of hardware.

10

3. A system for managing files, comprising:

sub-file storing means for storing one or a plurality of sub-files related to a main-file;

15        authentication information creating means for creating sub-file authentication information used to verify the sub-files; and

system file storing means for storing a system file to which the sub-file authentication information is related.

20

4. A system for managing files, comprising:

main-file storing means for storing a main-file;

authentication information creating means for creating main-file authentication information to be

25

used to verify the main-file; and

sub-file storing means for storing at least one sub-file to which the main-file authentication information is related.

5

5. A system for managing files, comprising:

main-file storing means for storing a main-file;

sub-file storing means for storing at least one sub-file to which the main-file authentication information is related;

10

authentication information creating means for creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

15

system file storing means for storing a system file to which the sub-file authentication information is related.

6. The system for managing files according to claim 5, wherein said main-file, said sub-files and said system files are stored in a non-secure area usually accessible.

20

7. The system for managing files according to claim 5, wherein said main-file, and said sub-files and said

25

09985677 110501

system files are stored in a non-secure area usually accessible and a secure area usually inaccessible, respectively.

5       8. The system for managing files according to claim 5, wherein said main-file and said sub-files, and said system files are stored in a non-secure area usually accessible and a secure area usually inaccessible, respectively.

10       9. The system for managing files according to claim 6, further comprising a computer and a storage unit, wherein

          the computer comprises  
15       reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

20       access allowing key storing means for storing the access allowing keys; and

          file accessing means for sending an access request together with the access allowing key,

          the storage unit comprises  
25       reciprocal authenticating means for reciprocally

09985677 110501

authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

5           access allowing key group storing means for storing all the access allowing keys; and

          access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing  
10   key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

          secure area accessing means for accessing a secure area usually inaccessible, and

15           the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the  
20   storage unit are reciprocally authenticated.

10. The system for managing files according to claim 7, further comprising a computer and a storage unit, wherein

25           the computer comprises

098867.10501  
FBI/DOJ

reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing all the access allowing keys; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually inaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

11. The system for managing files according to claim 8, further comprising a computer and a storage unit, wherein

the computer comprises reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing key; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing

keys;

access allowing key group storing means for storing all the access allowing keys; and

5 access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

10 secure area accessing means for accessing a secure area usually inaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the  
15 main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

12. The system for managing files according to claim  
20 9, wherein

the reciprocal authenticating means provided in said computer and said file accessing means are implemented by means of hardware.

25 13. The system for managing files according to claim



9, wherein

the medium ID is a card ID.

14. The system for managing files according to claim

5 9, wherein

the medium ID is a master ID.

15. The system for managing files according to claim

9, wherein

10 said authentication information is created for  
each record of a file.

16. The system for managing files according to claim

10, wherein

15 said authentication information is created for  
each record of a file.

17. The system for managing files according to claim

11, wherein

20 said authentication information is created for  
each record of a file.

18. A system for managing files, comprising:

25 sub-file reading means for reading one or a  
plurality of sub-files related to a main-file;

authentication information creating means for creating sub-file authentication information from sub-files read by the sub-file reading means;

5 system file reading means for reading sub-file authentication information from a system file related to the sub-file; and

10 authentication information comparing means for comparing the sub-file authentication information created by the authentication information creating means with the sub-file authentication information read by the system file reading means.

19. A system for managing files, comprising:

15 main-file reading means for reading a main-file; authentication information creating means for creating main-file authentication information from a main-file read by the main-file reading means;

20 sub-file reading means for reading main-file authentication information from sub-files related to the main-file; and

25 authentication information comparing means for comparing the main-file authentication information created by the authentication information creating means with the main-file authentication information read by the sub-file reading means.

20. A system for managing files, comprising:

main-file reading means for reading a main-file;

sub-file reading means for reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

system file reading means for reading sub-file authentication information from a system file related to the sub-file;

authentication information creating means for creating main-file authentication information from a main-file read by the main-file reading means and creating sub-file authentication information from sub-files read by the sub-file reading means; and

an authentication information comparing means for comparing the main-file authentication information created by the authentication information creating means with the main-file authentication information read by the sub-file reading means and comparing the sub-file authentication information created by the authentication information creating means with the sub-file authentication information read by the system file reading means.

21. The system for managing files according to claim

20, wherein said main-file, said sub-files and said system file are stored in a non-secure area usually accessible.

5 22. The system for managing files according to claim 20, wherein said main-file, and said sub-files and said system file are stored in a non-secure area usually accessible and a secure area usually inaccessible, respectively.

10 23. The system for managing files according to claim 20, wherein said main-file and said sub-files, and said system file are stored in a non-secure area usually accessible and a secure area usually  
15 inaccessible, respectively.

24. The system for managing files according to claim 21, further comprising a computer and a storage unit, wherein

20 the computer comprises  
reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing  
25 keys;

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key,

5 the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing  
10 keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the  
15 file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a  
20 secure area usually inaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file  
25 authentication information after the computer and the

storage unit are reciprocally authenticated.

25. The system for managing files according to claim  
22, further comprising a computer and a storage unit,  
5 wherein

the computer comprises

reciprocal authenticating means for reciprocally  
authenticating the computer with the storing unit and  
when the computer and the storage unit are  
10 reciprocally authenticated, creating access allowing  
keys;

access allowing key storing means for storing the  
access allowing key; and

file accessing means for sending an access  
15 request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally  
authenticating the storage unit with the computer and  
when the computer and the storage unit are  
20 reciprocally authenticated, creating access allowing  
keys;

access allowing key group storing means for  
storing all the access allowing keys; and

access allowing key identification means for  
25 identifying if the access allowing key sent from the

09985677 110501  
105077 12958660

file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

5        secure area accessing means for accessing a secure area usually inaccessible, and

         the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the  
10        main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

26. The system for managing files according to claim  
15        23, further comprising a computer and a storage unit, wherein

         the computer comprises

         reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and  
20        when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

         access allowing key storing means for storing all the access allowing keys; and

25        file accessing means for sending an access

00955677 4001

request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and  
5 when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

10 access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means,  
15 are the same; and

secure area accessing means for accessing a secure area usually inaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the  
20 secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

25 27. The system for managing files according to claim



24, wherein

the reciprocal authenticating means provided in said computer and said file accessing means are implemented by means of hardware.

5

28. The system for managing files according to claim 24, wherein

the medium ID is a card ID.

10

29. The system for managing files according to claim 24, wherein

the medium ID is a master ID.

15

30. The system for managing files according to claim 24, wherein

said authentication information is created for each record of a file.

20

31. The system for managing files according to claim 1, wherein

said secure area accessing means further comprises

access control information reading means for reading access control information stored in said secure area, and

25

009567-10500  
TOP SECRET

said storage unit further comprises

sector accessing means for accessing a main- file  
or sub-files related to the main-file in units of  
sectors or sector groups according to the access  
control information.

32. The system for managing files according to claim  
31, wherein

said secure area accessing means further  
comprises

access control information setting means for  
setting access control information in said secure  
area.

33. The system for managing files according to claim  
9, wherein

authentication information is created using one,  
two or all of said medium ID, said card ID and said  
master ID.

34. The system for managing files according to claim  
24, wherein

authentication information is created using one,  
two or all of said medium ID, said card ID and said  
master ID.

## 35. A computer, comprising:

reciprocal authenticating means for reciprocally authenticating the computer with a storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys; and

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key.

## 36. A storage unit, comprising:

reciprocal authenticating means for reciprocally authenticating the storage unit with a computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys;

access allowing key identification means for identifying if the access allowing key stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a

09985677-110501

secure area usually inaccessible.

37. A method of managing files, comprising the steps of:

- 5           reciprocally authenticating between a computer and a storage unit and when the computer and the storage unit are reciprocally authenticated, creating an access allowing key;
- storing the access allowing key;
- 10          storing all the access allowing keys;
- sending an access request together with the access allowing key;
- identifying if the access allowing key stored in the access allowing key storing step and at least one
- 15          access allowing key stored in the access allowing key group storing step, are the same; and
- accessing a secure area usually inaccessible.

38. A method of managing files, comprising the steps of:

- 20          storing one or a plurality of sub-files related to a main-file;
- creating sub-file authentication information used to verify the sub-files; and
- 25          storing a system file to which the sub-file

09955677-110501

authentication information is related.

39. A method of managing files, comprising the steps of:

- 5           storing a main-file;  
            creating main-file authentication information to  
be used to verify the main-file; and  
            storing at least one sub-file to which the  
main-file authentication information is related.

10

40. A method of managing files, comprising the steps of:

- storing a main-file;  
            storing at least one sub-file to which the  
15   main-file authentication information is related;  
            creating main-file authentication information to  
be used to verify the main-file/sub-file  
authentication information to be used to verify the  
sub-files; and  
20           storing a system file to which the sub-file  
authentication information is related.

41. A method of managing files, comprising the steps of:

- 25           reading one or a plurality of sub-files related

to a main-file;

creating sub-file authentication information from  
sub-files;

5 reading sub-file authentication information from  
a system file related to the sub-file; and

comparing the sub-file authentication information  
from the sub-files with the sub-file authentication  
information from the system file.

10 42. A method of managing files, comprising the steps  
of:

reading a main-file;

creating main-file authentication information  
from the main-file;

15 reading main-file authentication information from  
sub-files related to the main-file; and

comparing the main-file authentication  
information from the main-file with the main-file  
authentication information from the sub-file.

20

43. A method of managing files, comprising the steps  
of:

reading a main-file;

25 reading main-file authentication information from  
sub-files related to the main-file and one or a

plurality of sub-files related to the main-file;

reading sub-file authentication information from  
a system file related to the sub-file;

5 creating main-file authentication information  
from a main-file and creating sub-file authentication  
information from sub-files; and

10 comparing the main-file authentication  
information from the sub-file with the main-file  
authentication information from the main-file and  
comparing the sub-file authentication information from  
the system file with the sub-file authentication  
information from the sub-file.

15 44. A method of managing files, comprising the steps  
of:

reciprocally authenticating a computer with a  
storing unit and when the computer and the storage  
unit are reciprocally authenticated, creating access  
allowing keys; and

20 storing the access allowing keys; and

sending an access request together with the  
access allowing key.

25 45. A method of managing files, comprising the steps  
of:

reciprocally authenticating a storage unit with a computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

- 5       storing all the access allowing keys;
- identifying if the access allowing key and at least one access allowing key, are the same; and
- accessing a secure area usually inaccessible.

- 10      46. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

- 15       a reciprocal authenticating step of reciprocally authenticating between a computer and a storage unit and when the computer and the storage unit are reciprocally authenticated, creating an access allowing key;

- an access allowing key storing step of storing the access allowing key;

- 20       an access allowing key group storing step of storing all the access allowing keys;

- a file accessing step of sending an access request together with the access allowing key;

- an access allowing key identifying step of
    - 25      identifying if the access allowing key stored in the



access allowing key storing process and at least one access allowing key stored in the access allowing key group storing step, are the same; and

5 a secure area accessing step of accessing a secure area usually inaccessible.

47. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

10 sub-file storing step of storing one or a plurality of sub-files related to a main-file;

authentication information creating step of creating sub-file authentication information used to verify the sub-files; and

15 system file storing step of storing a system file to which the sub-file authentication information is related.

48. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

20 main-file storing step of storing a main-file; authentication information creating step of creating main-file authentication information to be used to verify the main-file; and

25

00985677 110501

sub-file storing step of storing at least one sub-file to which the main-file authentication information is related.

- 5 49. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file storing step of storing a main-file;

- 10 sub-file storing step of storing at least one sub-file to which the main-file authentication information is related;

authentication information creating step of creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

- 15 system file storing step of storing a system file to which the sub-file authentication information is related.

- 20 50. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

sub-file reading step of reading one or a plurality of sub-files related to a main-file;

- 25 authentication information creating step of

creating sub-file authentication information from sub-files;

system file reading step of reading sub-file authentication information from a system file related to the sub-file; and

authentication information comparing step of comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the system file.

51. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

authentication information creating step of creating main-file authentication information from a main-file;

sub-file reading step of reading main-file authentication information from sub-files related to the main-file; and

authentication information comparing step of comparing the main-file authentication information from the main-file with the main-file authentication information from the sub-file.

09985677 110501

52. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

5 sub-file reading step of reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

10 system file reading step of reading sub-file authentication information from a system file related to the sub-file;

15 authentication information creating step of creating main-file authentication information from a main-file and creating sub-file authentication information from sub-files; and

20 authentication information comparing step of comparing the main-file authentication information from the sub-file with the main-file authentication information from the main-file and comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the main-file.

25 53. A computer readable storage medium having a recorded file management program for enabling a

00955677 110501

computer to execute:

reciprocal authenticating step of reciprocally  
authenticating a computer with a storing unit and when  
the computer and the storage unit are reciprocally  
5 authenticated, creating access allowing keys; and

access allowing key storing step of storing the  
access allowing keys; and

file accessing step of sending an access request  
together with the access allowing key.

10

54. A computer readable storage medium having a  
recorded file management program for enabling a  
computer to execute:

reciprocal authenticating step of reciprocally  
15 authenticating a storage unit with a computer and when  
the computer and the storage unit are authenticated  
with each other, creating access allowing keys;

access allowing key group storing step of storing  
all the access allowing keys;

20 access allowing key identification step of  
identifying if the access allowing key and at least  
one access allowing key, are the same; and

secure area accessing step of accessing a secure  
area usually inaccessible.

25

0998567 110504